Compromising Emanations from USB 2 Interface

Leszek Nowosielski and Marian Wnuk
Faculty of Electronics, Military University of Technology
Gen. S. Kaliskiego 2 Str., Warsaw 00-908, Poland

Abstract— In the article assessment of the possibility of use and usability of USB 2.0 interface in IT devices used for classified information processing to minimize the risk of electromagnetic eavesdropping has been made. In those devices the aim is to minimize the level of radiated emissions via radio path, in which there is a high probability of interception by unauthorized persons and reproduction of conveyed information. The article has focused on revealing the possibility of eavesdropping of radiated compromising emanation during data transmission through USB 2.0 interface. For that purpose a comparative analysis of signal occurring directly on transmission line of USB 2.0 port has been made as well as its equivalent received by FSET 22 receiver as radiated emission. For the analysis signals generated by transmission lines of USB 2.0 port have been used. They were obtained as a result of measurements directly on transmission line and at the output of envelope detector of FSET 22 receiver received as radiated emission.

1. INTRODUCTION

Because of the fact that nowadays a big emphasis is put on classified information protection, modern IT devices and communication systems [10–13] are required not to pose a threat of interception of this kind of information. In this case loss of confidentiality might occur as a result of using electromagnetic emissions arising during operation of IT devices to intercept classified data. In this kind of devices a big emphasis is put on minimization of compromising emanation via radiated path. A particular threat of radiation of compromising signals via radio path is made by modern broad-band telecommunications interfaces such as: USB 2.0, USB 3.0, Ethernet etc.. In this study assessment of the possibility of use and usability of USB 2.0 interface in IT devices assigned for classified information processing has been made as well as a procedure of testing IT devices equipped with USB 2.0 interface has been suggested which aim is to assess the possibility of conducting electromagnetic eavesdropping of this type of devices.

2. OPTIMIZATION OF BINARY TESTING SEQUENCE FROM THE PERSPECTIVE OF MAXIMIZATION OF LEVEL OF RADIATED COMPROMISING EMANATION

A form of signal course directly on transmission line has a direct influence on the level of particular spectrum components of radiated emission from USB 2.0 received by eavesdropping receiver. That being so, for analyses aiming at assessment of the possibility of conducting electromagnetic eavesdropping, such a form of binary information sequences was selected which were generated by BTSG (binary testing sequence generator) transmission software operating at PC equipped with a tested USB 2.0 port, which results in maximization of a level of particular components of frequency spectrum of radiated emission. As a result of conducted tests and analyses it was determined that particular components of signal spectrum on USB 2.0 transmission line have maximal levels of particular spectrum components of radiated emission only for binary information sequences generated by BTSG, which after their processing by standard output systems of USB port generate periodic binary stream on transmission line. To force periodic binary stream on transmission line, BTSG should generate binary information sequence which after processing by standard output systems of USB 2.0 port will cause occurrence of periodic binary stream on transmission line.

Significant processes of signal processing in USB 2.0 interface, which have influence on a form of binary stream at its output include the process of bit stuffing and NRZI (non return to zero inverted) linear encoding. Taking into account the influence of the above methods of signal processing on the form of binary stream at output of USB 2.0 port, with the use of BTSG application it is necessary to transmit of the following binary information sequences through USB 2.0 interface:

- sequence of logic 0s: 000000000000000000. . . ,
- sequence of logic 1s: 1111111111111111. . . ,
- sequence of logic 1s and 0s: 010101010101010101. . . .

3. DETERMINATION OF DISTINCTIVE FEATURES OF SIGNALS OF RADIATED COMPROMISING

In order to show the possibility of electromagnetic eavesdropping during data transmission through USB 2.0 interface, measurements of signal spectrum occurring directly on USB 2.0 transmission line during transmission of information data sequence generated by BTSG described in the previous item of this article have been conducted. The measurements were carried out with the use of laboratory stand, which block diagram is presented in Fig. 1. An analysis of frequency spectra corresponding to particular sequences of information data generated by BTSG has allowed to define distinctive features such as frequencies characteristic for radiated compromising emanations generated by USB 2.0 port. In Fig. 2 a sample signal spectrum of radiated emission generated by USB 2.0 interface during transmission of information data sequence consisting of logic zeroes is presented. The conclusion resulting from the above spectrogram is that radiated compromising emanation occurs at frequencies: 240 MHz, 480 MHz and 720 MHz.

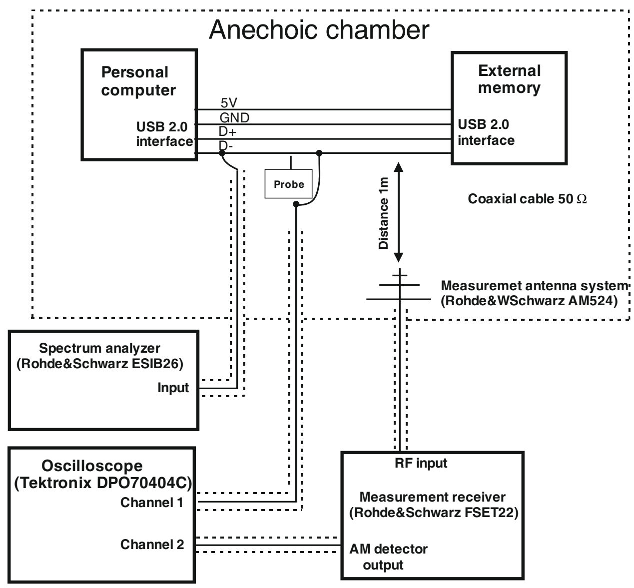

Figure 1: Block diagram of laboratory station for observation of signal occurring directly on transmission line of USB 2.0 port and its equivalent received by eavesdropping receiver as radiated emission.

In a further part of the experiment FSET 22 eavesdropping receiver was retuned to particular frequencies at which radiated compromising emanation occurs and then a comparative analysis of signal occurring directly on USB 2.0 transmission line and its equivalent received by eavesdropping receiver as radiated emission was made. For the comparative analysis signals generated by USB 2.0 port were used. They were received as a result of measurements directly on transmission line and at the output of envelope detector of FSET 22 receiver as radiated emission. A sample display of oscillograms matching information data sequence generated by BTSG consisting of logic zeroes is presented in Fig. 3. The analysed time courses and their spectra were obtained as a result of measurements conducted at measuring position, which block diagram is presented in Fig. 1. After an initial comparative analysis large similarity of signals recorded directly on transmission line of USB 2.0 port can be noticed (oscillogram of yellow colour in Fig. 3) as well as its equivalent received by eavesdropping receiver as radiated emission(oscillogram of green colour in Fig. 3). The result of the above observation proves the possibility of electromagnetic eavesdropping.

In Table 1 distinctive frequencies occurring during transmission of particular sequences of information data generated by BTSG was presented on which large correlation of signals occurring directly on USB 2.0 transmission line was found as well as at the output of envelope detector of FSET 22 receiver received as radiated emission.

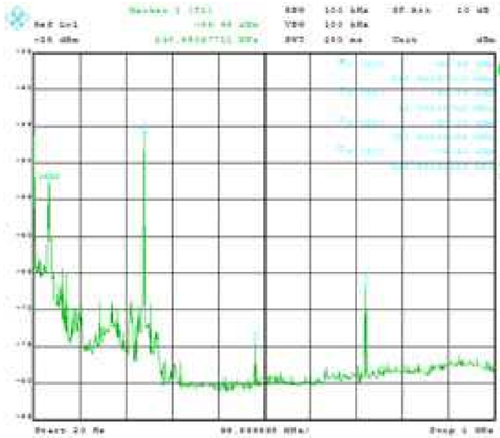

Figure 2: Frequency spectrum of signal during transmission of logic zeroes.

Figure 3: Oscillogram for USB 2.0 interface during transmission of information data sequence consisting of logic zeroes. Yellow colour — directly from interface transmission line. Green colour — signal at output of amplitude detector of eavesdropping receiver tuned to frequency $f = 240\,\text{MHz}$.

Table 1: Distinctive frequencies for compromising emanation generated by USB 2.0 port.

Information data sequence generated by FG	...111111...	...000000...	...010101...
Distinctive frequencies for compromising emanation generated by USB 2.0 port.	34.29 MHz, 68.58 MHz, 102.87 MHz	240 MHz, 480 MHz, 720 MHz	120 MHz, 240 MHz, 360 MHz,

4. ASSESSMENT OF DEGREE OF ELECTROMAGNETIC LEAKAGE FROM USB 2.0 INTERFACE

In order to assess a degree of electromagnetic leakage from USB 2.0 interface a degree of similarity between signal generated by USB 2.0 port received as a result of measurements directly on transmission line and at the output of envelope detector of FSET 22 receiver received as radiated emission was calculated. The degree of similarity was calculated for signals recorded during transmissions of particular test sequences of information data generated by BTSG discussed in the second item of this article. As a measure of the leakage degree correlation coefficient was used. On the basis of the studies it has been found that selection of an appropriate number of analysed signal samples for calculating correlation coefficient has a significant influence on their value. In Table 2 dependence of correlation coefficient value of signal recorded directly on transmission line of USB 2.0 interface has been presented as well as for signal recorded at the output of envelope detector of FSET 22 receiver received as radiated emission in the function of signal sample amount. For the analysed signals the biggest value of correlation coefficient was obtained for 8000 signal samples.

Table 2: Dependence of correlation coefficient value of signal recorded directly on transmission line of USB 2.0 interface and for signal recorded at the output of envelope detector of FSET 22 receiver received as compromising emanation in the function of signal sample amount.

Item no.	**Number of samples**	**Correlation coefficient**
1	500	0,6245
2	5000	0,6980
3	8000	0,6967

5. CONCLUSIONS

The article has focused on showing the possibility of electromagnetic eavesdropping during data transmission through USB 2.0 interface. For that purpose the comparative analysis of signal occurring directly on transmission line of USB 2.0 port has been made as well as its equivalent received by FSET 22 receiver as radiated emission. The conclusion from the conducted analyses is that:

- Using USB 2.0 interface for data transmission poses a threat of electromagnetic eavesdropping, which negates the possibility of its usability in IT devices used for classified information processing without using additional protections.
- A form of signal course directly on transmission line has a direct influence on the level of particular spectrum components of radiated emission from USB 2.0 port received by eavesdropping receiver. That being so, for testing IT devices equipped with USB 2.0 interface aiming at assessment of possibilities of conducting electromagnetic eavesdropping it is necessary to select such a form of binary information sequences generated by BTSG transmission software operating on PC equipped with a tested USB 2.0 port, which results in maximization of the level of particular components of frequency spectrum of radiated emission. Such sequences include binary sequences consisting of: logic zeroes, logic ones and alternate sequences of logic ones and zeroes.
- Binary information sequence generated by BTSG transmission line in the form of sequence of logic zeroes causes radiated emission with maximal levels of particular components of frequency spectrum.
- Correlation coefficient between signal recorded at the output of envelope detector of eavesdropping receiver FSET 22 as radiated emission and signal recorded directly on transmission line of USB 2.0 interface can be successfully used as similarity measures between the above mentioned signals during tests of IT devices equipped with USB 2.0 interface aiming at assessment of possibilities of conducting electromagnetic eavesdropping.
- The radio path attenuation have a big influence on the compromising emanation level. The attenuation can estimated using the radio-wave propagation modelling [1–9].

ACKNOWLEDGMENT

The project is financed from NCBiR means within the Agreement No. 0024/R/ID2/2012/02 in the years 2012–2015.

REFERENCES

1. Kubacki, R., J. Ferenc, and R. Przesmycki, "The measurements of the complex permittivity and permeability of powdered nanocrystalline Fe-Si-B-Cu-Nb ("Finemet")," *Przeglad Elektrotechniczny*, Vol. 87, No. 12B, 92–95, 2011.
2. Kubacki, R., E. Cwalina, M. Kuchta, and A. Dukata, "Electromagnetic field distribution in the office room and computer enclosure evoked by electromagnetic high power pulses," *Przeglad Elektrotechniczny*, Vol. 88, No. 12B, 209–212, 2012.
3. Kubacki, R., "Biological interaction of pulse-modulated electromagnetic fields and protection of humans from exposure to fields emitted from radars," *2008 MIKON Conference Proceedings*, Vol. 1 and 2, 66–72, 2008.
4. Kubacki, R., J. Sobiech, and E. Sedek, "Model for investigation of microwave energy absorbed by young and mature living animals," *Electromagnetic Field, Health and Environment, Proceedings of EHE'07, Studies in Applied*, Vol. 29, 126–132, 2008.
5. Kubacki, R., J. Kieliszek, and A. Krawczyk, "The investigation of influence of the electromagnetic fields emitted from short-wave diathermy to the pacemakers," *Przeglad Elektrotechniczny*, Vol. 83, No. 12, 105–107, 2007.
6. Kubacki, R., J. Sobiech, J. Kieliszek, and A. Krawczyk, "Comparison of numerical and measurement methods of SAR of ellipsoidal phantoms with muscle tissue electrical parameters," *COMPEL — The International Journal for Computation and Mathematics in Electrical and Electronic Engineering*, Vol. 25, No. 3, 691–704, 2006.
7. Dabrowski, M. P., W. Stankiewicz, R. Kubacki, E. Sobiczewska, and S. Szmigielski, "Immunotropic effects in cultured human blood mononuclear cells pre-exposed to low-level 1300 MHz pulse-modulated microwave field," *Electromagnetic Biology and Medicine*, Vol. 22, No. 1, 1–13, 2003.

8. Kubacki, R., M. Krukowski, J. Kieliszek, and J. Sobiech, "New computational model of electromagnetic field distribution for predicting of the safety zones in the near-field of microwave antennas," *XIV International Conference on Microwaves, Radar and Wireless Communications, MIKON-2002*, Vol. 1–3, 902–905, 2002.
9. Michalak, J. and B. Uljasz, "Relative efficiency of broadcasting in the cluster based network — Simulation results," *Military Communications and Information Systems Conference (MCC 2013)*, Francja, Saint-Malo, Jun. 10–Jul. 8, 2013, ISBN 978-83-62954.
10. Piotrowski, Z., "Angle phase drift correction method effectiveness," *Signal Processing Algorithms, Architectures, Arrangements, and Applications Conference Proceedings*, 82–86, 2009, ISBN: 978-83-62065-00-4.
11. Byłak, M. and D. Laskowski, "Assessment of network coding mechanism for the network protocol stack 802.15.4/6LoWPAN," *Advances in Intelligent Systems and Computing, Springer International Publishing AG*, Switzerland, Vol. 224, 75–82, 2013, ISSN: 2194–5357 (Print), 2194–5365 (Online).
12. Laskowski, D., P. Łubkowski, and M. Kwasniewski, "Identification of suitability services for wireless networks," *Przeglad Elektrotechniczny*, R. 89 9/2013, Sigma-Not, Warszawa, str. 128-132, 2013, ISSN 0033-2097.
13. Byłak, M. and D. Laskowski, "Diagnosis coding efficiency of network coding mechanism for wireless networks," *Przeglad Elektrotechniczny*, R. 89 9/2013, Sigma-Not, Warszawa, str. 133-138, 2013, ISSN 0033-2097.